Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132
Telephone: none
Email: none

Daniel David Rigmaiden
Pro Se, Defendant

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

United States of America, Plaintiff, v. Daniel David Rigmaiden, et al., Defendant.	No. CR08-814-PHX-DGC SECOND SUPPLEMENT TO MOTION TO SUPPRESS RE: SEARCH AND SEIZURE OF DIGITAL EVIDENCE UNDER N.D.Cal. WARRANTS

Defendant, Daniel David Rigmaiden, appearing *pro se*, respectfully submits *Second Supplement To Motion To Suppress RE: Search And Seizure Of Digital Evidence Under N.D.Cal. Warrants*.[1] Based on the **newly provided June 21, 2012 evidence**,[2] the newly provided **October 22, 2012 evidence**,[3] and new legal authority that the defendant was

1. This filing was originally a "first" supplement (Dkt. #867) and is now a "second" supplement that will likely be updated again as a "third" supplement considering the government continues with its four year long protracted discovery process and is yet to sufficiently comply with the defendant's July 5, 2012 discovery request. *See also Reply To Government's Response To Motion For Discovery RE: Digital Evidence Search* (Dkt. #930).

2. The newly provided June 21, 2012 evidence, as well as other prior evidence recently made relevant by the newly provided evidence, is attached to the defendant's *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues* (Dkt. #863).

3. The newly provided October 22, 2012 evidence, as well as other prior evidence recently made relevant by the newly provided evidence, is attached to the defendant's *Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues* (Dkt. #929) and *Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues* (Dkt. #933).

unable to bring to the Court's attention earlier,[4] this supplemental filing seeks to supplement and supersede prior arguments made in the defendant's *Motion To Suppress* (Dkt. #824), and incorporated *Memorandum Re: Fourth Amendment Violations (re: N.D.Cal. 08-70460-HRL/PVT)* (Dkt. #830-1), regarding the search and seizure of digital evidence contained on the defendant's physical data storage devices seized from 431 El Camino Real, Apartment No. 1122, Santa Clara, CA 95050 (hereafter "apartment No. 1122"). The arguments in this filing address constitutional violations and two separate technical violations applicable to the N.D.Cal. 08-70460-HRL/PVT warrant and (now applicable) N.D.Cal. 08-70502-PVT warrant.[5]

The defendant's filings at Dkt. #824 and #830-1 reference his prior assumption that IRS-CI Agent Daun made her initial search and seizure of data—by copying files from forensic images of the defendant's data storage devices to DVDs and a CD—within 30 days of the physical search of apartment No. 1122. Although not specifically discussed at Dkt. #824 and #830-1, the defendant was also under the impression that government actors had employed keyword searches or other means that would limit "human eye" exposure to *out-of-scope* data, as required by the relevant warrants. However, after filing Dkt. #824 and #830-1, the government provided the defendant with new evidence indicating that IRS-CI Agent Daun initially took 401 days to search and seize data from the images of the defendant's storage devices seized under the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants. According to the N.D.Cal. warrants, the final day IRS-CI Agent Daun was permitted to search and seize data from the images was September 2, 2008 (08-70460-HRL/PVT) and September 3, 2008 (08-70502-PVT) but her search/seizure of data was not complete until September 8, 20**09**. Furthermore, after filing Dkt. #824 and #830-1, the

---

4. *See* United States v. Collins, Case No. 11-CR-00471-DLJ (PSG), Doc. #328 (N.D.Cal., Aug. 27, 2012).

5. The defendant's filings at Dkt. #824 and #830-1 did not originally challenge the search and seizure of digital evidence stemming from the N.D.Cal. 08-70502-PVT warrant used to search storage unit No. A-47, CBD Indoor Mini, 570 Cinnabar Street, San Jose, California, 95110 (hereafter "storage unit No. A-47"). However, as outlined in this filing, the newly discovered technical violation merits a direct challenge to the N.D.Cal. 08-70502-PVT warrant.

government provided new evidence indicating that IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray were also engaged in exploratory rummaging through clones of the defendant's entire computer system for approximately one year after the physical search of apartment No. 1122. Furthermore, after filing Dkt. #824 and #830-1, the government provided new evidence indicating that various government actors failed to employ means designed to "locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[6] and instead used their "human eyes" to review a multitude of the defendant's private *out-of-scope* data for an extended period of time. As outlined below, the above explained newly provided evidence changes the facts of the case and the defendant's arguments with respect to the government's search and seizure of digital data. The defendant now needs to update and supersede his prior wholesale suppression argument (*see* Dkt. #830-1) in light of the newly provided evidence and he also needs to raise new challenges relating to the newly identified technical violations of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants. The proceeding sections provide supplemental, corrected, and superseded facts, arguments, and concluding section as specified in the *'d paragraphs.

I. FACTS: supplemental, corrected, and superseded with respect to the government's seizure of digital data.

*. In light of the new evidence provided to the defense by the government on June 21, 2012 and on October 22, 2012, the following facts supplement, correct, and supersede the facts contained in the defendant's *Motion To Suppress* (Dkt. #824), *Memorandum Re: Fourth Amendment Violations* (Dkt. #824-1), *General Facts*, Section IV(B)(17), ¶ Nos. 86-88, which were incorporated into the *Memorandum Re: Fourth Amendment Violations (re: N.D.Cal. 08-70460-HRL/PVT)* (Dkt. #830-1) and applicable to the arguments contained therein.

1. On August 3, 2008, the government searched apartment No. 1122 while

6. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

executing the "AMENDED" version of the N.D.Cal. 08-70460-HRL/PVT warrant.[7] During the search, the government physically seized the defendant's home computer, physical data storage devices, encrypted virtual drives, and other various physical evidence in the possession of the defendant. During the physical search of the defendant's home and in the months[8] following the search, IRS-CI Agent Daun imaged the defendant's data storage devices and encrypted virtual drives by mirroring/copying them to government hard drives.[9][10] Likewise, the data storage device and encrypted virtual drive seized from storage unit No. A-47, during the August 4, 2008 execution of the N.D.Cal. 08-70502-PVT warrant,[11] were imaged by IRS-CI Agent Daun in the same fashion.[12]

2. Once the seized data storage devices and encrypted virtual drives were imaged, IRS-CI Agent Daun began what would end up being a 401-day exploratory rummaging through the defendant's files contained on his home computer, data storage devices, and encrypted virtual drives. According to the October 22, 2012 prosecution report, IRS-CI Agent Daun would not complete her search and seizure of data from the forensic images and

---

7. *See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30, 2008* (Dkt. #464-1, p. 20) (return).

8. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 8) (table with "1/9/2009" entry marking the last DriveCrypt encrypted virtual drive that was imaged).

9. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Tracy L. Daun stating that she conducted a partial live acquisition of the defendant's "T" drive using WinRAR and imaged the remainder of the drives using IXimager).

10. Throughout this filing, when the defendant refers to "forensic images" or similar and "encrypted virtual drives" or similar, said terms also encompass the government's live acquisition of the defendant's "T" drive into a WinRAR archive—which is the same as creating a mirror copy of the drive sans preservation of file access dates—and all files contained therein, both within and beyond the scope of the N.D.Cal. 08-70460-HRL/PVT warrant. *See id*.

11. *See Submission Of Documents Related To Original Northern District Of California 08-70502-HRL Search Warrant Used To Physically Search Storage Unit No. A-47* (Dkt. #846-2).

12. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1, p. 29-36) (IRS-CI Agent Daun discussing physical data storage device and encrypted virtual drive seized from storage unit No. A-47).

virtual machine clones[13] until September 8, 2009[14]—371 days past the 30-day deadline for search/seizure of data as permitted by the N.D.Cal. 08-70460-HRL/PVT warrant[15] and 370 days past the 30-day deadline for search/seizure of data as permitted by the N.D.Cal. 08-70502-PVT warrant.[16]

3. In addition to taking 401 days to *complete* her forensic analysis, IRS-CI Agent Daun took nearly **six months** to even *begin* her forensic analysis of the DriveCrypt encrypted virtual drives corresponding to "filesalot.dcv," "filesalot_bak_3-1-2008.dcv," and "filesalot_bak_3-31-2008.dcv"[17]—the drives containing the bulk of the digital *in-scope* evidence seized from the defendant. Likewise, IRS-CI Agent Daun took more than **nine months** to even *begin* her forensic analysis of the WinRAR live acquisition image of the "T" drive, *i.e.*, "T_drive.rar".[18] Although IRS-CI Agent Daun and the other case agents began arbitrarily rummaging through virtual machine clones of the defendant's entire computer system immediately after the physical drives were seized, the forensic analyses intended to determine whether any irrelevant, personal information was improperly seized was not

---

13. FYI, "encrypted virtual drives" are different from "virtual machine clones."

14. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 9) (table with "8/14/2009 through 9/8/2009" entry stating "Prepared reports and extracted files from the analysis on the computer media.").

15. *See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (Dkt. #566-2, p. 16) ("The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and **no later than thirty (30) calendar days** after the initial execution of the warrant." (emphasis added)).

16. *See Submission Of Documents Related To Original Northern District Of California 08-70502-HRL Search Warrant Used To Physically Search Storage Unit No. A-47*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (Dkt. #846-2, p. 8) ("The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and **no later than thirty (30) calendar days** after the initial execution of the warrant." (emphasis added)).

17. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 8) (table with "2/2/2009," "2/13/2009," and "3/1/2009" entries indicating the dates IRS-CI Agent Daun began her forensic analysis of the defendant's DriveCrypt encrypted virtual drives).

18. *See id.*, EXHIBIT 01 (Dkt. #929-1, p. 9) (table with "5/20/2009" entry stating "Started analysis on WinRAR live acquisition ran onsite at search warrant.").

started for **any** imaged drive until February 2, 2009.[19]

4. In order to facilitate the seizure of data at the conclusion of her initial 401-day exploratory rummaging, IRS-CI agent Daun searched through the forensic images, extracted all files that fell within the scope of the warrants, and then copied some of those files to DVDs and a CD so that they would be isolated (*i.e.*, seized) from the images. This forensic search process, occurring off and on between February 2, 2009 and September 8, 2009, took **219 days** even while IRS-CI Agent Daun admitted that she could have been finished in roughly **60 days**, *i.e.*, "by late March or early April."[20] IRS-CI Agent Daun had plenty of free time to complete her forensic analysis from the start, however, she instead opted to spend the first 33 days, *i.e.*, August 3, 2008 through September 4, 2008,[21] creating virtual machine clones of the defendant's entire computer system to facilitate the untrained exploratory rummaging of three other case agents.[22] Apart from the three other case agents, the actual process of searching and seizing the defendant's digital data **through a forensic analysis** is explained in IRS-CI Agent Daun's "Computer Forensic Report," originally provided to the defense via discovery on February 25, 2010.[23]—more than **six months** after the report's completion on September 8, 2009. The "Computer Forensic

---

19. *See id.*, EXHIBIT 01 (Dkt. #929-1, p. 8).

20. *See Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #933-1); A review of the entries in the October 22, 2012 table also support IRS-CI Agent Daun's claim of being *capable* of completing the analysis within **60 days**. IRS-CI Agent Daun's February 27, 2009 admission completely undermines the prosecution's recent claim that "the length of time that the United States has spent analyzing the lawfully seized material is reasonable in light of the amount of incriminating data seized[.]" *Government's Response To Defendant's Motion To Suppress* (Dkt. #873, p. 66).

21. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 8) (table with 8/3/2008 through 9/4/2008 entries detailing the time IRS-CI Agent Daun devoted to creating the virtual machine clones instead of conducting the forensic analysis).

22. If IRS-CI Agent Daun had a legitimate excuse for being unable to conduct a timely search, she could have provided some or all physical drives to the FBI's Computer Analysis Response Team (CART)—consisting of personnel trained in digital forensics—considering the FBI was actively involved in the investigation.

23. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

Report" states under numerous "Analysis" headings that, "The following is a summary of the evidence located on the computer that fell within the parameters of the Search Warrant and the Items to be Seized."[24]

5. As for the files copied/seized by IRS-CI Agent Daun to the CD and DVDs as *in-scope*, the amount of files falling within the scope of the relevant warrants was only a small fraction of the total number of files contained within the forensic images of the defendant's data storage devices and encrypted virtual drives. For examples, under the "Analysis - T_drive.rar (WinRAR archive)" heading of her "Computer Forensic Report," IRS-CI Agent Daun indicated that she seized a total of 3205 files[25] while the "live acquisition" image (*i.e.*, the WinRAR archive) contains a total of 26,983 files. In other words, 88.12 % of the files contained in the WinRAR archive image of the "T" drive are beyond the scope of the relevant warrant. The following table displays additional file seizure ratios applicable to various (but not all) data storage devices and encrypted virtual drives that were imaged by IRS-CI Agent Daun:[26]

Storage Device Or Encrypted Virtual Drive:	Warrant Relevant To Physical Seizure:	Number Of Files Seized From Images:	Total Number Of Files On Drive:	Percentage Of Imaged Files Beyond Scope Of Warrant:
Analysis - IBM ThinkPad (S/N LV-C4398)	N.D.Cal. 08-70460-HRL/PVT (**apartment**)	590	60,891	**99.03 %**
Analysis - T_drive.rar (WinRAR archive)	N.D.Cal. 08-70460-HRL/PVT (**apartment**)	3205	26,983	**88.12 %**
Analysis - "filesalot.dcv"	N.D.Cal. 08-	3281	53,520	**93.87 %**

24. *See id.*, EXHIBIT 01 (Dkt. #863-1, p. 30).

25. *See id.*, EXHIBIT 01 (Dkt. #863-1, p. 11-15).

26. The values contained in the "Number Of Files Seized From Images" column of the table were calculated by adding together the total number of seized files listed under the relevant "Analysis" heading contained in the "Computer Forensic Report." *See id.*, *passim*. The values contained in the "Total Number Of Files On Drive" column were calculated by using the ESTsoft ALZip program or Microsoft Windows Explorer program to determine how many files were within the relevant forensic image applicable to each drive. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 10, EXHIBIT 11, EXHIBIT 12, EXHIBIT 13, and EXHIBIT 14 (screenshots of file/folder or archive properties dialog box relevant to each forensic image) (Dkt. #863-1).

	70460-HRL/PVT (**apartment**)			
Analysis - "filesalot_bak_3-1-2008"	N.D.Cal. 08-70460-HRL/PVT (**apartment**)	2244	51,353	**95.63 %**
Analysis - "filesalot_bak_3-31-2008"	N.D.Cal. 08-70502-PVT (**storage unit**)	2784	51,734	**94.62 %**

6. Although the N.D.Cal. 08-70460-HRL/PVT warrant and N.D.Cal. 08-70502-PVT warrant each state that the 30-day deadline for searching and seizing digital data "may be extended by court order for good cause shown[,]"[27] the government made no applications to the issuing magistrate or other magistrate to extend the deadlines to search and seize digital data past 30 days. The government's initial 401-day fishing exhibition was entirely unauthorized.

7. During IRS-CI Agent Daun's 401-day fishing exhibition into images and virtual machine clones of the defendant's data storage devices and encrypted virtual drives, which the government admits "actually contain many more files than those that fall within the parameters of the Search Warrant and its attachments[,]"[28] IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray also had access to their own virtual copies of the defendant's entire computer system,[29] as provided to them by IRS-CI Agent

---

27. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, Application, Warrant*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (Dkt. #566-2, p. 17).

28. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47, p. 31).

29. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 03 (Dkt. #863-1) (August, 2009 emails between IRS-CI Agent Tracy L. Daun *et al.*: detailing that IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray all had their own virtual machine clones of the defendant's computer system up to at least **August 30, 2009**); *see also Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 3) ("The virtual machines each consisted of the IBM thinkpad computer, the 100GB external hard drive found in the apartment, the 500GB external hard drive found in the apartment and the 100GB external hard drive found in the storage unit."). The report also states that "[n]o other computer media seized from the search warrants were accessible through the virtual

Daun as early as August 31, 2008.[30] The agents' "virtual machines" allowed them to access clones of the defendant's home computer and all files, including the DriveCrypt encrypted virtual drives,[31] as if sitting in front of the defendant's actual powered-on computer and data storage devices.[32] In other words, at least three additional case agents engaged in a year long exploratory rummaging through the defendant's files[33] while the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants only allowed 30-day examinations. It was only after IRS-CI Agent Daun completed her initial 401-day search and seizure of data from the forensic images (by copying data to DVDs and a CD)[34] that she instructed the other agents to stop accessing the defendant's computer system and files.[35] IRS-CI Agent Daun's

---

machines." *Id*. However, this claim is both irrelevant and misleading. First, all other seized physical media were either blank or contained commercially available software, *i.e.*, installation CDs. *See id.*, EXHIBIT 02 (Dkt. #929-1, p. 14) (noting Windows Vista CDs, camera and GPS memory cards, OS recovery CDs, blank CDs, *etc.*). Second, the physical drive clones accessible via the virtual machines contain full copies of all DriveCrypt encrypted virtual drives—even those containing only *out-of-scope* data. *See also* fn. No. 31, *infra*.

30. *See id.*, EXHIBIT 01 (Dkt. #929-1, p. 8) (table entry dated "8/31/2008" reading "Cloned VM for case agent use").

31. The "virtual machines" created by IRS-CI Agent Daun contain precisely the **same data** as the "forensic images." For example, the first noted 100GB external hard drive contains the DriveCrypt encrypted container file, "filesalot.dcv," which can be decrypted and mounted as an encrypted virtual drive within the virtual machine. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues* EXHIBIT 01 (Dkt. #863-1, p. 16) ("Computer Forensic Report" by IRS-CI Agent Daun indicating that "filesalot.dcv" is contained on the 100GB external hard drive which is, in turn, contained within virtual machine clones). Additionally, each virtual machine copy allows the user to access a clone of the operating system running on the defendant's laptop, which includes the ability to run installed programs and analyze the installed environment.

32. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 04 (Dkt. #863-1) (August 10, 2008 email from IRS-CI Agent Daun to AUSA Battista *et al.*: IRS-CI Agent Daun explaining that "[a] virtual machine allows me to sit there and view [][the defendant's] computer, as if I was actually sitting at his computer[.]").

33. The number of occurrences any given government actor accessed the virtual machine clones will likely forever remain a mystery due the government's failure to preserve evidence. *See Motion To Suppress All Digital Data Evidence As A Sanction For Failure To Preserve Evidence* (Dkt. #931); *see also Reply To Government's Response To Motion For Discovery RE: Digital Evidence Search*, Section I(C) (Dkt. #930).

34. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

35. *See id.*, EXHIBIT 03 (Dkt. #863-1) (August 2009 emails between IRS-CI Agent Tracy

instruction to cease the fishing exhibition came on August 28, 20**09**[36]—more than a year after the physical search of apartment No. 1122.

8. At the time IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray were arbitrarily rummaging through virtual machine clones of the defendant's entire computer system, not one of them had been previously trained in computer forensic investigations.[37] Unlike IRS-CI Agent Daun who failed to apply her training on avoiding exposure to *out-of-scope* data, the other case agents began their year long exploratory rummaging knowing they had no relevant training at all. Rather than operate within a computer forensics environment, the other case agents accessed all of the defendant's data, including *out-of-scope* data, "as if [][they] w[ere] actually sitting at his computer"[38] over the course of a year.

9. As a general matter, IRS-CI Agent Daun is not shy about admitting her willingness to intentionally delay a search and seizure if doing so serves an unrelated side purpose that benefits the activities of other agents. While inside the defendant's residence on August 3-4, 2008, IRS-CI Agent Daun took the time to image more than 100 gigabytes of data in order to, in her own words, give other agents time "to get a follow up warrant for

---

L. Daun *et al.*: IRS-CI Agent Daun advising the primary case agents that, "[a]t this point, no one should be viewing the virtual machines.").

36. *See id*.

37. *See e.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122, Warrant*, "Computer Search Protocol For The Northern District Of California," *Application* (Dkt. #566-1, p. 4-5) (explaining training and experience of IRS-CI Agent Medrano and IRS-CI Agent Fleischmann); *id.*, (Dkt. #566-1, p. 18) (explaining training and experience of FBI Agent Murray). Note: FBI Agent Murray's computer crime training is very different from computer forensic investigations training. *See*, *e.g.*, Daniel, Larry and Daniel, Lars, *Digital Forensics For Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, (Waltham, MA: Syngress Publications, 2012), p. 13 (As for seized digital data, "[t]he analysis phase is also where the greatest disparity begins to become a factor between the skills and approach of a 'computer expert' and those of a computer or digital forensics expert. While a computer expert may understand many aspects of computer usage and data, a properly trained forensic expert will be well versed in recovering data as well as in proper examination techniques.").

38. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 04 (Dkt. #863-1).

some additional items in the apartment."[39] IRS-CI Agent Daun conducted this needless and lengthy on-site imaging even while she planned to "seiz[e] everything - including the items [][she] imaged..." anyways.[40] Rather than simply seize the physical drives and image them off-site, as permitted by the N.D.Cal. 08-70460-HRL/PVT warrant, IRS-CI Daun's intentional foot-dragging allowed other agents to hang-out in the defendant's home for 27 hours.[41] Hardly requiring a 27-hour search, the defendant's home is only 489 *ft*^{2},[42] contained minimal possessions,[43] and was clean and orderly.[44]

10. Even after IRS-CI Agent Daun completed her 371-day late search and seizure of data from the defendant, and even after IRS-CI Agent Daun's August 28, 2009 instruction that, "[a]t this point, no one should be viewing the virtual machines[,]"[45] she still continued her personal exploratory rummaging into the forensic images at least until January 1, 2012,[46] *i.e.*, an additional 28 months following the September 8, 2009 creation of the noted CD and DVDs. For example, IRS-CI Agent Daun re-accessed the original images (*i.e.*, the encrypted virtual drives containing "many more files than those that fall within the

---

39. *Id.*, EXHIBIT 05 (Dkt. #863-1) (August 7, 2008 email from IRS-CI Agent Daun to Jeffrey H. Willert).

40. *Id*.

41. *See id.*, EXHIBIT 06 (Dkt. #863-1) (IRS report of search warrant execution at apartment No. 1122).

42. *See First Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 29 (Dkt. #587-2) (Domicilio apartments floor plans showing studio apartment at 489 *ft*^{2}); *id.*, EXHIBIT 30 (Dkt. #587-2) (Domicilio apartments site map showing apartment No. 1122 to be a studio apartment).

43. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 07 (Dkt. #863-1) (August 6, 2008 email from FBI Agent Murray to FBI supervisor: apartment No. 1122 was sparse, clean, and orderly).

44. *See id*.

45. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 03 (Dkt. #863-1).

46. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 9) (table indicating that IRS-CI Agent Daun reaccessed the forensic images on "1/12/2012" to extract data for the prosecution).

parameters of the Search Warrant and its attachments[]")[47] in October of 2011.[48][49] While re-accessing the forensic images, IRS-CI Agent Daun copied the file "agj_bag_liner_jagbags.co.nz.txt"—a file not even listed in her original "Computer Forensic Report."[50] After becoming aware of the defendant's planned Fourth Amendment challenges around March of 2012, the prosecution instructed IRS-CI Agent Daun to cease her re-accessing of the forensic images and virtual machine clones, which contain *out-of-scope* data, and to stop her copying/seizing of additional files into evidence.[51]

11. While conducting her more than three year long exploratory rummaging into the defendant's data, IRS-CI Agent Daun did not employ means designed to "locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[52]—as was required by the applicable "Computer Search Protocol." Instead, IRS-CI Agent Daun used her "human eyes" to review a multitude of the defendant's files—**possibly all of them**—in order to determine which files

---

47. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47, p. 31).

48. *See id.*, EXHIBIT 08 (Dkt. #863-1) (government discovery providing "agj_bag_liner_jagbags.co.nz.txt" (seized from forensic image of the defendant's data storage device) containing personal communications between the defendant (under his alias of Andrew Johnson) and Jacqueline Gardiner).

49. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 088 (Dkt. #821-5, p. 37) (March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored Information by IRS-CI Agent Daun, stating that the "agj_bag_liner_jagbags.co.nz.txt" file was obtained in October of 2011).

50. *See id*, EXHIBIT 088 (Dkt. #821-5, p. 38) (March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored Information by IRS-CI Agent Daun, stating that "[t]he above file [agj_bag_liner_jagbags.co.nz.txt] is located in a DriveCrypt encrypted volume named filesalot.dcv on the Toshiba 100GB hard drive... The agj_bag_liner_jagbags.co.nz.txt file **is not individually listed in the analysis reports.**" (emphasis added)).

51. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 9) (table with "3/7/2012" entry stating "Resubmitted report to AUSA from 12/16/2012 request to only include files that were included in initial analysis completed September 2009").

52. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122*, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

qualified as *in-scope* data.[53] IRS-CI Agent Daun conducted her abrasive "human eye" review even after determining in August of 2008 that the defendant used very descriptive and accurate file/folder labeling for all *in-scope* document data.[54] The defendant's practice of precisely naming the noted *in-scope* files to reflect content was so extensive and accurate that IRS-CI Agent Daun included the full file paths corresponding to *in-scope* data she provided to an FBI computer programmer considering she believed the defendant's detailed and accurate file/folder labeling would be helpful to the programmer's analysis of the data.[55] Rather than extract *in-scope* files based on the defendant's descriptive and accurate file/folder labeling, and/or based on extensive use of keyword searches, and/or through some other means, IRS-CI Agent Daun opted for file-by-file, "human eye" exploratory rummaging and employed only rare keyword searches to locate credit card numbers.[56]

12. Although the prosecution now claims that during her "human eye" review IRS-CI Agent Daun "ignored" any file falling outside the scope of the relevant warrants,[57] various emails sent by IRS-CI Agent Daun tell otherwise. For example, IRS-CI Agent Daun's "human eye" exploratory rummaging allowed her to learn that the defendant had an interest in outdoor activities, vitamins, and nutrition[58]—interests having nothing to do with

---

53. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 7) ("Her main search consisted of reviewing files and making determinations whether the file fell within the scope of the warrant. If the file did appear to fall within the scope of the warrant, she marked it for inclusion in her final report. If it did not appear to fall within the scope of the warrant, she ignored the file.").

54. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 04 (Dkt. #929-1, p. 21) (IRS-CI Agent Daun noting that the defendant "tended to be kind of descriptive" with file and folder names corresponding to data responsive to the relevant warrants.). As a purely hypothetical example, if the defendant had a text file on his computer that contained IRS tax code, he would have named the file/folder something like "T:\information\taxes\IRS_tax_code.txt".

55. *See id*.

56. As noted by the prosecution, the only keyword searches used by IRS-CI Agent Daun —which were notably "rare"—consisted of credit card numbers. *See id.*, EXHIBIT 01 (Dkt. #929-1, p. 7).

57. *See id.*, EXHIBIT 01 (Dkt. #929-1, p. 7) ("If the file did appear to fall within the scope of the warrant, she marked it for inclusion in her final report. If it did not appear to fall within the scope of the warrant, **she ignored the file**." (emphasis added)).

58. *See id.*, EXHIBIT 03 (Dkt. #929-1, p. 18) (At the time of her extended 3-year+ search

the crimes alleged or evidence listed in the relevant warrants. Rather than ignore the *out-of-scope* files relating to outdoor activities, vitamins, and nutrition, IRS-CI Agent Daun **shared her knowledge** with the prosecution and even posited that she collect those *out-of-scope* files for AUSA Battista's personal review.[59] Complete knowledge gleaned from the various government actors conducting "human eye" reviews of the defendant's *out-of-scope* data may never be known due to the government's failure to preserve evidence pertaining to what files each government actor "looked at."[60]

13. The one of many files accessed by IRS-CI Agent Daun after September 8, 2009, *i.e.*, "agj_bag_liner_jagbags.co.nz.txt," contains personal communications between the defendant[61] and Jacqueline Gardiner.[62] Similar to the data relating to outdoor activities, vitamins, and nutrition, the information contained in the file is not relevant to the charges against the defendant and the government has provided no explanation as to how the file helps its case. In fact, in response to an inquiry regarding IRS-CI Agent Daun's belated seizure of "agj_bag_liner_jagbags.co.nz.txt," AUSA Battista informed the defendant that government "[s]earches for evidence to be used in this case are being limited to the materials indexed in the February 25, 2010, discovery."[63] The February 25, 2010 discovery referred to by AUSA Battista is IRS-CI Agent Daun's September 8, 2009 "Computer Forensic Report;"[64] corresponding to the later provided CD and DVDs which do not contain

---

in December of 2011, IRS-CI Agent Daun asked AUSA Frederick A Battista, "Do you care about the purchase of the outdoor equipment / clothes? Vitamins /nutritional stuff?").

59. *See id*.

60. *See Motion To Suppress All Digital Data Evidence As A Sanction For Failure To Preserve Evidence* (Dkt. #931); *see also Reply To Government's Response To Motion For Discovery RE: Digital Evidence Search*, Section I(D) (Dkt. #930).

61. The defendant's communication was under his alias of Andrew Johnson. *See* declaration RE: *Daniel Rigmaiden owns the aircard and used the aircard service as a home Internet connection*, ¶ 4, p. 2 (Dkt. #824-3) (explaining that the defendant used the alter ego of "Andrew Johnson").

62. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 08 (Dkt. #863-1) ("agj_bag_liner_jagbags.co.nz.txt").

63. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 088 (Dkt. #821-5) (March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored Information by IRS-CI Agent Daun).

64. *See Third Submission Of Consolidated Exhibits Relating To Discovery And*

"agj_bag_liner_jagbags.co.nz.txt."[65] The government has provided no explanation for IRS-CI Agent Daun's and other agents' non-stop—more than three year long—exploratory rummaging through the defendant's personal files that hold no relevance to the government's case and are outside the scope of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

II. ARGUMENT: supplemental, corrected, and superseded with respect to the government's seizure of digital data.

*. In light of the new evidence provided to the defense by the government on June 21, 2012 and on October 22, 2012, and in light of new legal authority issued in *Collins*, the following arguments supplement, correct, and supersede the arguments contained in the defendant's *Motion To Suppress* (Dkt. #824), *Memorandum Re: Fourth Amendment Violations (re: N.D.Cal. 08-70460-HRL/PVT)* (Dkt. #830-1), *Argument*, Section II(C). However, arguments relating to the defendant's reasonable expectation of privacy in his data contained on his hard drives, encrypted virtual drives, and the forensic images / virtual machine clones created therefrom—as they are in the possession of the government—established in the defendant's *Motion To Suppress* (Dkt. #824), *Memorandum Re: Fourth Amendment Violations* (Dkt. #824-1), *Argument*, Section V(C)(10), remain unchanged/unaffected and, pursuant to LRCiv 7.1(d)(2) when referenced through LRCrim 12.1, are hereby incorporated into this filing by reference.

A. Wholesale suppression is merited considering case agents turned the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants into general warrants while flagrantly disregarding their terms.

The government's unauthorized, more than three year long, "human eye" exploratory rummaging through the defendant's digital data merits wholesale suppression of all evidence

---

Suppression Issues, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

65. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 088 (Dkt. #821-5) (March 7, 2012 IRS Memorandum for Transmittal of Electronically Stored Information by IRS-CI Agent Daun wherein IRS-CI Daun admits that "agj_bag_liner_jagbags.co.nz.txt" is not listed in her analysis reports).

seized under the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants[66] or, at the very least, wholesale suppression of all seized digital evidence. "[W]here there is a 'flagrant disregard' for the terms of the warrant, the district court may suppress all of the evidence, including evidence that was not tainted by the violation." United States v. Chen, 979 F.2d 714, 717 (9th Cir. 1992) (citing United States v. Medlin, 842 F.2d 1194, 1199 (10th Cir. 1988))); *see also* United States v. Sears, 411 F.3d 1124, 1131 (9th Cir. 2005) ("Wholesale suppression is an extraordinary remedy that is appropriate only when the officers transform the search into an impermissible general search by ignoring the terms of the warrant and engaging in indiscriminate fishing." (internal quotation marks and citation omitted)). In the subsections that follow, the defendant will explain how the case agents flagrantly disregarded the time limitations and minimization terms contained in the N.D.Cal. warrants' "Computer Search Protocol"[67] in order to advance a more than three year long fishing exhibition into the defendant's digital data. The subsections that follow will also show that the government's misconduct resulted in prejudice in the form of unnecessary exposure to private *out-of-scope* data and indiscriminate sharing of information gleaned from that data.

1. The government facilitated its fishing exhibition by flagrantly disregarding the 30-day search window term contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

The relevant N.D.Cal. warrants dictated exactly how the government was to search the data storage devices seized from apartment No. 1122 and storage unit No. A-47. The

66. As explained in the facts above, the government's exploratory rummaging also applied to the images of the data storage device and encrypted virtual drive seized from storage unit No. A-47 during execution of the N.D.Cal. 08-70502-PVT warrant. However, as long as the defendant successfully argues for *wholesale* suppression of all digital evidence seized in the context of the N.D.Cal. 08-70460-HRL/PVT warrant, all digital and physical evidence seized from storage unit No. A-47 would also be suppressed considering the N.D.Cal. 08-70502-PVT warrant stemmed from digital evidence seized under the N.D.Cal. 08-70460-HRL/PVT warrant, *i.e.*, a fruit-of-the-poisonous-tree. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 05 (Dkt. #863-1) (explaining how a text file seized from an encrypted virtual drive seized from apartment No. 1122 led to the search of storage unit No. A-47).

67. The government has effectively seized **all** of the data contained on the defendant's physical data storage devices and encrypted virtual drives even while it knows that most of the data is beyond the scope of the relevant warrants. At best, the government was only authorized to preserve digital evidence but this does not mean that agents can continue to rummage through preserved digital evidence over a three year period while it is intermingled with data not within the scope of the warrants.

warrants required that the government "complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and no later than thirty (30) calendar days after the initial execution of the warrant[,]"[68] unless a time extension is obtained from the court "for good cause shown."[69] Instead of completing her search and seizure of data within 30 days as required by the warrants, or seeking extensions of time from the issuing magistrates, IRS-CI Agent Daun forestalled even *beginning* her forensic analysis of the forensic images for six months[70] – an analysis intended to determine whether any irrelevant, personal information was improperly seized. In *Metter*, the court found that the government may not "seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of that data to determine whether any irrelevant, personal information was improperly seized."[71] Rather than *begin* the forensic analysis, let alone complete it, IRS-CI Agent Daun spent the first 33 days[72] creating and then sharing a virtual machine clone of the defendant's entire computer system with IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray.[73] The three noted case agents used their virtual machines to arbitrarily rummage through the defendant's personal files—most of which are beyond the scope of the warrant—for approximately one year.[74] Likewise, IRS-CI Agent Daun conducted her initial fishing exhibition via the virtual machines for approximately six months and then via the forensic images for

---

68. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No. 1122*, *Warrant*, ¶ 5, p. 2 (Dkt. #566-2, p. 16).

69. *Id.*, ¶ 5 (Dkt. #566-2, p. 17).

70. *See Facts*, Section I, ¶ No. 3, *supra*.

71. United States v. Metter, No. 10-CR-600 (DLI), Doc. 219, p. 16 (E.D.N.Y., May 17, 2011) ("The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable."). Notably, the *Metter* court found a Fourth Amendment violation even while the applicable warrant had no express time limitation like the warrants relevant in the present case.

72. *See Facts*, Section I, ¶ No. 4, *supra*.

73. *See Facts*, Section I, ¶ No. 7, *supra*.

74. The three noted case agents received their virtual machine clones as early as August 31, 2008 and were instructed by IRS-CI Agent Daun to stop accessing them on August 28, 20**09**. *See id*.

approximately seven months.[75] The later seven month forensic search process, occurring off-and-on between February 2, 2009 and September 8, 2009, took **219 days** even while IRS-CI Agent Daun admitted that she could have been finished in roughly **60 days**, *i.e.*, in her own words, "by late March or early April."[76] Still out for the catch, IRS-CI Agent Daun then continued with an additional 28 month long fishing exhibition into the defendant's private *out-of-scope* data via repeated re-accessing of her copy of the virtual machine clone and forensic images.[77] Sometime in March of 20**12**, after becoming aware of the defendant's plan to challenge IRS-CI Agent Daun's and other agents' misconduct, AUSA Battista finally gave an instruction to IRS-CI Agent Daun to cease re-accessing the virtual machine clone and forensic images and to only access the *in-scope* data seized to her September 8, 2009 CD and DVDs.[78] As icing on the cake, the prosecution took more than six months, *i.e.*, until February 25, 2010, to even provide the defendant with a copy of the "Computer Forensic Report" and list of files copied/seized completed by September 8, 2009.[79]

The directive contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants, requiring that all digital evidence be searched and seized from the forensic images within 30 days unless an extension of time is granted, is intended to ensure, among other protections, that the issuing magistrate supervise a protracted search so as to prevent exploratory rummaging through files not within the scope of the warrant. Not only did IRS-CI Agent Daun and other agents flagrantly disregard the plain terms of the warrants, their

---

75. *See Facts*, Section I, ¶ Nos. 3-4, *supra*.

76. *See Facts*, Section I, ¶ No. 4, *supra*. IRS-CI Agent Daun's February 27, 2009 admission completely undermines the prosecution's recent claim that "the length of time that the United States has spent analyzing the lawfully seized material is reasonable in light of the amount of incriminating data seized[.]" *Government's Response To Defendant's Motion To Suppress* (Dkt. #873, p. 66). Further contradicting the government's claim, the October 22, 2012 prosecution report indicates that IRS-CI Agent Daun took one to three calendar days to examine most of the forensic images. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 8-9).

77. *See Facts*, Section I, ¶ No. 10, *supra*.

78. *See id*.

79. *See id*.

doing so resulted in the type of protracted exploratory rummaging the warrants intended to prevent. Unlike the situations in *Ivers*[80] and *Hill*,[81] IRS-CI Agent Daun's delay was first motivated by a desire to advance the fishing exhibition by creating virtual machine clones for the other untrained[82] case agents—a process of which she **devoted the first 33 days**[83] following the physical searches. Even if one were to assume a busy schedule, IRS-CI Agent Daun made no attempt to lighten her workload by providing physical drives to the available FBI unit specifically trained in digital forensic investigations.[84] IRS-CI Agent Daun not "want[ing] to have to eat [][her] words!"[85] in the "IRS-CI vs. FBI" agency rivalry may have played a role in her decision to not take advantage of available resources in the multi-agency investigation. In any event, there was neither permission nor justification for IRS-CI Agent Daun and three additional untrained agents to violate the terms of the warrants by conducting an initial 401-day fishing exhibitions into virtual machine clones of the defendant's computer system while it "actually contain[ed] many more files than those that fall within the parameters of the Search Warrant and its attachments."[86] Likewise, IRS-CI Agent Daun's thereafter additional 28-month long personal fishing exhibition, which

---

80. *Compare* United States v. Ivers, 430 F. App'x 573 (9th Cir. 2011) ("Given the circumstances of this case [(which involved a warrant with no express time limits)] and the nature of the seized materials, the FBI acted diligently and offered a reasonable explanation for any delay," *i.e.*, "the FBI prioritized based on legitimate public policy concerns." (footnote omitted)).

81. *Compare* United States v. Hill, 459 F.3d 966, 977 (9th Cir. 2006) ("Because the officers were motivated by considerations of practicality rather than by a desire to engage in indiscriminate fishing, we cannot say that the officers so abused the warrant's authority that the otherwise valid warrant was transformed into a general one, thereby requiring all fruits to be suppressed" (citations and markup omitted)).

82. *See Facts*, Section I, ¶ No. 8, *supra* (explaining how the other case agents were not trained in computer forensic investigations).

83. *See Facts*, Section I, ¶ No. 4, *supra*.

84 *I.e.*, the FBI Computer Analysis Response Team (CART).

85. *Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 02 (Dkt. #933-1) ("the AUSA didn't believe that the IRS had the resources to do this and wanted to bring the FBI in. He also thought their CART people were better suited for this. We stood up for ourselves and I don't want to have to eat my words! :-)").

86. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

occurred after she instructed other agents to stop rummaging through the defendant's files, was also done without permission or justification. The above explained inexcusable, unauthorized, and illegitimately motivated delays support the defendant's claim of exploratory rummaging and indiscriminate fishing.

In *Collins*, the Court denied a motion to suppress after addressing a government "failure to comply with the warrant as to a separate time line which had been established for **creation of**... **a mirror image** of the computer contents – which was an anticipated means for carrying out a forensic examination of the computer."[87] The Court in *Collins* denied the motion to suppress because the subsequent **search** "was completed within th[e] time [specified] and was in full compliance with the terms of the Search Warrant."[88] However, the 30-day search window violation at issue in the present case is clearly distinguishable. Unlike the defendant in *Collins*, this defendant is not pushing the government's failure to create forensic images in a timely manner—a separate violation altogether. Rather, he is challenging the government's failure to complete the actual **search** within the time frames specified in the relevant warrants. The violation at issue here is much more severe considering it involves the actual **search** as opposed to a ministerial action of simply mirroring the seized physical drives and DriveCrypt encrypted virtual drives. The court in *Collins* denied the motion to suppress because "[t]he timing violation affects a mechanism used for the search, it does not affect the search itself."[89] In the present case, the government's exploratory rummaging was conducted well beyond the 30-day time frames and clearly affected the search itself by turning it into a general search.

2. The government facilitated its fishing exhibition by flagrantly disregarding the minimization terms contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

Evidence of indiscriminate fishing is firmly established by the first 401-day multi-agent search—which occurred mostly outside of a computer forensics environment—and the

87. United States v. Collins, Case No. 11-CR-00471-DLJ (PSG), Doc. #328, p. 6 (N.D.Cal., Aug. 27, 2012) (emphasis added).

88. *Id.*

89. *Id.* at p. 7.

thereafter 28-month search by IRS-CI Agent Daun, both involving unauthorized government rummaging through virtual machine clones and forensic images that "actually contain many more files than those that fall within the parameters of the Search Warrant and its attachments."[90] However, further exacerbating the fishing exhibition, government actors also failed to employ means designed to "locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[91] First, while not being trained on how to segregate and avoid exposure to *out-of-scope* data,[92] IRS-CI Agent Medrano, IRS-CI Agent Fleischmann, and FBI Agent Murray used their virtual machine clones to arbitrarily rummage through the defendant's personal files. "Failing to follow accepted best practices leaves the work of the forensic examiner open to challenge and the possibility of the evidence collected being suppressed."[93] Rather than use EnCase or AccessData FTK,[94] which have numerous tools to assist examiners in limiting exposure to *out-of-scope* data,[95] the three noted case agents conducted their arbitrary rummaging as if they were actually sitting at the defendant's powered-on computer over the course of a full year.[96] Second, IRS-CI Agent Daun did not

---

90. *See id*.

91. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

92. Unlike IRS-CI Agent Daun, the noted case agents did not have computer forensic investigations training and were otherwise not trained on how to avoid exposure to private *out-of-scope* data intermingled with *in-scope* data. *See Facts*, Section I, ¶ No. 8, *supra*.

93. Daniel, *Digital Forensics For Legal Professionals*, p. 26. "Certifications for persons in the field, [][are] the EnCase Certified Examiner (EnCE), the Computer Certified Examiner (CCE), the Access Certified Examiner (ACE), the Computer Forensics Certified Examiner (CFCE), and the GIAC Certified Forensic Analyst (GCFA), to name a few[.]" *Id.*, p. 25.

94. *See* Guidance Software [website], *EnCase Forensic - Computer Forensic Data Collection for Digital Evidence Examiners*, http://www.guidancesoftware.com/encase-forensic.htm (last accessed: Nov. 19, 2012); AccessData Group [website], *Computer Forensics Software for Digital Investigations*, http://www.accessdata.com/products/digital-forensics/ftk (last accessed: Nov. 19, 2012).

95. For example, AccessData FTK has advanced search features that include stemming, phonic, synonyms, related, and fuzzy, which intelligently locate misspelled words and typos. AccessData FTK also has culling features including filters and facets designed to locate only *in-scope* data.

96. *See Facts*, Section I, ¶ No. 8, *supra*.

begin accessing the forensic images using EnCase until six months after the start of her own arbitrary rummaging via her copy of the virtual machine clone.[97] Third, while finally conducting her forensic analysis, IRS-CI Agent Daun continued to use her "human eyes" to review a multitude of the defendant's files—**possibly all of them**—in order to locate *in-scope* data to copy to her CD and DVDs.[98] IRS-CI Agent Daun utterly failed to "expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[99] IRS-CI Agent Daun conducted her total "human eye" review even after discovering early on that the defendant was meticulous in accurately and precisely labeling relevant file and folder names to reflect the *in-scope* data content of any given file.[100] Likewise, IRS-CI Agent Daun opted for a "human eye" review rather than make extensive use of the EnCase and/or AccessData FTK keyword search feature and other modern day technology[101] which would have identified only the files that were *in-scope* while shielding those that were *out-of-scope*. Fourth, the defendant has suffered prejudice in the form of government actors exposing themselves to *out-of-scope* data/information and then sharing it with others.[102] The following subsections provide a detailed analysis of the above points in light of relevant case law.

a Keywords searches are adequate for complying with a warrant's express minimization requirements.

In *Lu*, the government at least attempted to comply with a warrant's **express** minimization requirements—identical to those at issue here—by only conducting keyword searches to locate *in-scope* data. *See* United States v. Fu-Tain Lu, No. CR-09-00341 RMW, Doc. No. 112, p. 4 (N.D.Cal., Sept. 16, 2010). The court in *Lu* found that "the method used

97. *See Facts*, Section I, ¶ No. 3, *supra*.

98. *See Facts*, Section I, ¶ Nos. 11-13, *supra*.

99. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

100. *See Facts*, Section I, ¶ No. 11, *supra*.

101. *See id*.

102. *See Facts*, Section I, ¶ Nos. 8 & 11-14, *supra*.

by Agent Zaborowski, assuming he made appropriately narrow word searches, [means that] only those documents that had a likelihood of being within the scope of the warrant were examined by human eyes. Thus, potential Fourth Amendment concerns were minimized." *Id.* at p. 5. In the present case, "the only keywords used were to find credit card numbers"[103] and IRS-CI Agent Daun instead used her "human eyes" to manually look at a multitude of the defendant's files in order to determine if any given file fell within the scope of the warrant.[104] In *Lu*, the court assumed narrow keyword searches and denied the motion to suppress but granted discovery with respect to what files were "looked at" so the defense would have an opportunity to file for "reconsideration if [][it] discovers that the Government did a search of the mirror images that was not reasonably designed to find only documents, files or data described in the warrant[.]" *Id*. In the present case, the defendant does not have a list of precisely which files were "looked at" because keyword searches were not employed and the government failed to preserve a list of "human eye" reviewed files.[105] However, based on the October 22, 2012 prosecution report,[106] the defendant presumes that **all** files were looked at using "human eyes," which is a reasonable presumption given how long the fishing exhibition lasted and given the wording used in the report. The government looking at **all** of the defendant's files, over a very long period of

---

103. *Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 7). Note: the defendant has no qualm with the government conducting adequately narrow keyword searches (of data content) to identify *in-scope* files and thereafter using "human eyes" to view the matching files to confirm that they are in fact *in-scope*. However, skipping right to an arbitrary "human eye" review of a multitude of files—as was done by IRS-CI Agent Daun—is a blatant Fourth Amendment violation and also a violation of the "Computer Search Protocol" contained in the relevant warrants.

104. IRS-CI Agent Daun conducted her extensive "human eye" review of the contents of a multitude of the defendant's files even while realizing early on that the defendant "tended to be kind of descriptive" with file and folder names corresponding to data responsive to the relevant warrants. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 04 (Dkt. #929-1, p. 21). *See also Facts*, Section I, ¶ No. 11, *supra*.

105. *See Motion To Suppress All Digital Data Evidence As A Sanction For Failure To Preserve Evidence* (Dkt. #931); *see also Reply To Government's Response To Motion For Discovery RE: Digital Evidence Search*, Section I(D) (Dkt. #930).

106. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 7).

time, supports the defendant's claim of exploratory rummaging and indiscriminate fishing.

b The government could have conducted an effective search while at the same time protecting the defendant's privacy interests.

Contrary to some other cases,[107] and in light of the express minimization terms of the warrants, the defendant need not posit any effective alternative search method considering file-by-file, "human eye" review is the epitome of doing absolutely **nothing** in terms of limiting agent exposure to *out-of-scope* data. Although no specific guidelines were provided, the relevant warrants required that the government do *something* and by doing *nothing* the government clearly violated the warrants' minimization terms. However, if the Court requires suggestions, there are numerous alternatives to abrasive, file-by-file "human eye" review that could have been employed. For example, aside from employing available minimization technology, the government could have began by **not** passing around virtual machine clones of the defendant's entire computer system, which allowed numerous unqualified government actors to access *out-of-scope* data outside the forensic environment. In any event, the case agents could have stopped using their "human eyes" to review data content once it was determined in August of 2008 that the defendant accurately labeled his files and folders containing the *in-scope* data.[108] At that point, there was no longer any suspicion of the defendant "do[ing] all [][he could] to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from

107. *See* United States v. Burgess, 576 F.3d 1078, 1095 (10th Cir. 2009) ("Burgess complains the particular methodology used in this case was over broad, yet he offers no alternative methodology that would protect his legitimate interests and also permit a thorough search for evidence of drug trafficking."); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) (defendant did not suggest "how the search in this case would have been different with a scripted search protocol.").

108. *See Facts*, Section I, ¶ No. 11, *supra*.

the casual observer." Hill, 459 F.3d at 978.[109] Unlike in *Adjani*,[110] a case where the Ninth Circuit rejected a defendant's self-labeling argument, IRS-CI Agent Daun not only lacked a reason to not "trust the suspect's self-labeling," 452 F.3d at 115, she **relied upon** said labeling to increase the efficiency of the FBI's investigation into computer code.[111] Had the government also used the defendant's accurate labeling as a means to only "examine[] suspicious and out-of-place folders," it would have more effectively "engaged in a focused search of the hard drives rather than a general search." United States v. Stabile, 633 F.3d 219, 239-40 (3rd Cir. 2011). However, even if not reasonable to rely upon the defendant's confirmed accurate labeling, AccessData FTK has the ability to identify files via header analysis, conduct OCR conversions, and facilitate sophisticated keyword searches. *See infra*.

As for minimization technology available at the time of the initial physical searches and continuing through the government's more than three year long fishing exhibition, there were numerous tools available that the government could have used to conduct an effective search while also meeting the requirement to "expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant..."[112] Addressing a computer forensic search using early 20**03** technology, the Ninth Circuit in *Giberson* upheld file-by-file, "human eye" review but "acknowledge[d] that new technology may become readily accessible to enable more efficient or pinpointed

---

109. Rather than employ phony file/folder names and file extensions, the defendant employed DriveCrypt encrypted virtual drives of which IRS-CI Agent Daun was able to access as soon as she sat down at the defendant's computer. *See Government's Response To Defendant's Motion To Suppress* (Dkt. #873, p. 26) ("Fortunately for the investigation team,... [w]hen entry was made pursuant to the search warrant, [the] defendant's computer was found to be unsecured and logged on, no password was needed in this instance in order to access the files."); *Fourth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 14 (Dkt. #898-1) (**August 25, 2008** email from IRS-CI Agent Daun to AUSA Battista: "I was able to image each of the items and feel pretty confident that I have gotten around the encryption issue.").

110. United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006).

111. *See Facts*, Section I, ¶ No. 11, *supra*.

112. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

searches of computer data, and that, if so, we may be called upon to reexamine the technological rationales that underpin our Fourth Amendment jurisprudence in this technology-sensitive area of the law." United States v. Giberson, 527 F.3d 882, 890 (9th Cir. 2008) (markup and citation omitted) [addressing a warrant with **no** minimization requirements]. For the July, 20**08** searches approved by courts having jurisdiction over the technology capital of the planet,[113] it is objectively reasonable[114] to conclude that the warrants contemplated use of some of the so-called new technology in order to comply with the express minimization requirements. Society's prior technological limitations may have once provided justification for courts to not "restrict[] the search... to specific search terms, [considering doing so] would likely have failed to cast a sufficiently wide net...,"[115] however, in late 2008 there were a number of software tools available that could have been used to effectively employ *in-scope* keyword searches and similar minimization methods contemplated by the warrants. First, copies of image files such as a PDFs, JPGs, GIFs, BMPs, and TIFFs could have been converted using Optical Character Recognition (OCR) software so that all text, handwriting, markings (*e.g.*, barcodes), and graphics were searchable.[116] Running an imaged based document through OCR and then conducting

113. *I.e.*, Silicon Valley.

114. "Fourth Amendment reasonableness is predominantly an objective inquiry.... This approach recognizes that the Fourth Amendment regulates conduct rather than thoughts; and it promotes evenhanded, uniform enforcement of the law." Ashcroft v. al-Kidd (al-Kidd II), 131 S.Ct. 2074, 2080 (2010).

115. Adjani, 452 F.3d at 1149-50. Note: the warrant in *Adjani*, which was executed in the context of January 20**04** technology, did not contain express minimization requirements like the warrants at issue in the present case. Furthermore, this defendant is not advocating any "specific search terms" like the defendant did in *Adjani*. *See Lu*, No. CR-09-00341 RMW, Doc. No. 112 (not applying *Adjani* and accepting **government chosen** keyword searches as an adequate minimization method – subject to later review as to reasonableness).

116. *See*, *e.g.*, Wikipedia [website], *Optical character recognition – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Optical_character_recognition (last accessed: Nov. 15, 2012) ("**Optical character recognition**, usually abbreviated to OCR, is the mechanical or electronic conversion of scanned images of handwritten, typewritten or printed text into machine-encoded text."); Wikipedia [website], *Sketch recognition – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Sketch_recognition (last accessed: Nov. 15, 2012); Wikipedia [website], *Handwriting recognition – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Handwriting_recognition (last accessed: Nov. 15, 2012) (Note: rather than detect characters, targeted keyword matching increases accuracy by reducing the problem domain – for example, automatic handwritten postal address recognition used by the USPS – which is perfect for a targeted handwritten keyword

keyword searches eliminates problems that arise, for example, when a documents is "in 'tiff' format," or a "'digital picture of a hard copy document' that has been scanned[.]"[117] Second, in order to determine if *in-scope* sound data is hidden within commercial music mp3 audio, the government could have used the CDDB database[118] to authenticate/verify "full CD" mp3 folders or used technology from SoundHound, Inc.[119] to authenticate/verify any given individual mp3. Speaker-independent speech recognition could have then been applied to all suspect mp3 files in order to match audio data segments corresponding to all possible targeted spoken keywords.[120] Similar image/speech analysis methods apply to videos in AVI and other formats, which are all just combinations of still images and audio tracks.[121] Third, in order to detect misspelled words, typos, and code words corresponding to targeted keywords, the government could have expanded each keyword search to include

---

computer forensic search); Wikipedia [website], *Computer vision – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Computer_vision (last accessed: Nov. 15, 2012) ("**Content-based image retrieval** – finding all images in a larger set of images which have a specific content. The content can be specified in different ways, for example in terms of similarity relative to a target image (give me all images similar to image X), or in terms of high-level search criteria given as text input (give me all images which contains many houses, are taken during winter, and have no cars in them).").

117. United States v. Evanson, 2007 WL 4299191, p. 5 (D. Utah Dec. 5, 2007).

118. *See* Wikipedia [website], *CDDB – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/CDDB (last accessed: Nov. 15, 2012) ("CDDB was designed around the task of identifying entire CDs, not merely single tracks. The identification process involves creating a 'discid', a sort of 'fingerprint' of a CD created by performing calculations on the track duration information stored in the table-of-contents of the CD []. This discid is used with the Internet database, typically either to download track names for the whole CD or to submit track names for a newly-identified CD.").

119. *See* SoundHound, Inc. [website], *SoundHound Inc.*, "About Us," http://www.soundhound.com/index.php?action=s.about (last accessed: Nov. 16, 2012) ("SoundHound's breakthrough Sound2Sound technology searches sound against sound, bypassing traditional sound to text conversion techniques even when searching text databases.").

120. *See* Wikipedia [website], *Speech recognition – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Speech_recognition (last accessed: Nov. 15, 2012) ("In 2006, Google published a trillion-word corpus[.]"); Wikipedia [website], *Speech analytics – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Speech_analytics (last accessed: Nov. 16, 2012).

121. *See*, *e.g.*, Daniel, *Digital Forensics For Legal Professionals*, p. 21 ("Digital video and photo forensics are grouped together for a reason. A photo is a still image, and a video is a sequence of still images. When you watch a video, it is a sequence of still images changing so fast that it appears as continuous movement.").

misspelled/typo/code variants – as listed in any number of "misspelled word databases" like those used by the Google search engine and by Wikipedia.[122][123][124] For example, searching "Jug Davi G. Camell" on the Google search engine automatically corrects to "Judge David G. Campbell,"[125] *i.e.*, detecting the typos and using a proximity analysis to convert the codeword "Jug" to "Judge." In the event of "human eye" review being unavoidable for any given file, the case agents could have either (1) had a neutral and walled-off third-party conduct the forensic analysis of the target file with instructions to return only *in-scope* data to the case file, or (2) sought judicial authority to ignore the express minimization requirements. Because the defendant has suggested both technology based and non-technology based ways of how an effective forensic analysis could have been conducted in compliance with the warrants' minimization requirements, cases such as *Burgess* and *Giberson* cannot be used to belittle the warrants' terms and reject the defendant's arguments.[126]

c The defendant has been prejudiced by the government's failure to comply with minimization requirements.

The government's failure to conduct a forensic examination designed to "expose only those categories of files, documents, or other electronically stored information that are

---

122. *See* Wikipedia [website], *Wikipedia:List of common misspelling – Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Wikipedia:List_of_common_misspellings (last accessed: Nov. 15, 2012).

123. *See also* Dumbtionary [website], *Dumbtionary.com a dictionary of misspelled words*, http://www.dumbtionary.com (last accessed: Nov. 16, 2012) ("Just type the correct word above with a plus sign (+) before it and if misspellings are available they will be shown. If no misspellings are available, check back soon because we will find them and add them.").

124. *See also* fn. No. 99 (AccessData FTK has on-the-fly misspelled/typo/code word keyword search capability).

125. *Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 03 (Dkt. #933-1) (google search engine result for "Jug Davi G. Camell").

126. One may counter that "human eye" review cannot be avoided due to the possibility of criminals inventing new and innovative ways to hide *in-scope* data in seemingly innocuous *out-of-scope* digital files. However, the same is true for paper documents. For example, there is always a possibility that a suspect will use tiny microprint to hide a drug ledger within his medical records or a *Sir Francis Bacon* open code system to hide evidence of insider trading within a series of love letters. However, those mere possibilities have never justified the government taking a microscope to an *out-of-scope* medical file or sending a box of *out-of-scope* love letters to a cryptanalyst.

identified with particularity in the warrant..."[127]—during the more than three year long fishing exhibition—also resulted in identifiable prejudice to the defendant. Overall, the government's lengthy, indiscriminate, "human eye" rummaging resulted in government actors collecting and sharing the defendant's private *out-of-scope* data and information gleaned therefrom. For example, IRS-CI Agent Daun seized the file "agj_bag_liner_jagbags.co.nz.txt" in October of 2011. The file at issue contains personal communications between the defendant and Jacqueline Gardiner. The prosecution has already admitted that "agj_bag_liner_jagbags.co.nz.txt" will not be used as evidence considering it is not amongst the list of data falling within the scope of the warrant. AUSA Battista indicated that "[s]earches for evidence **to be used in this case** are being limited to the materials indexed in the February 25, 2010, discovery[,]"[128] *i.e.*, various reports listing specific files seized by IRS-CI Agent Daun **not** including "agj_bag_liner_jagbags.co.nz.txt." The fact that the government continues an ongoing search through the forensic images, *etc.* for the purpose of seizing data not responsive to the N.D.Cal. 08-70460-HRL/PVT warrant —or even relevant to **this case**—is an additional indication that the unauthorized fishing exhibition was/is anything but harmless. As another example, IRS-CI Agent Daun exposed herself to enough *out-of-scope* data to learn of the defendant's interests in outdoor activities, vitamins, and nutrition.[129] IRS-CI Agent Daun then shared her *out-of-scope* knowledge with AUSA Battista and posited that she obtain the relevant files for his personal review.[130] Even if the Court were to find the warrants' minimization terms trivial and accept as constitutional some form of indiscriminate, file-by-file, "human eye" review,[131] IRS-CI

---

127. *E.g.*, *Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California" (Dkt. #566-2, p. 17).

128. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 088 (Dkt. #821-5) (emphasis added).

129. *See Facts*, Section I, ¶ No. 12, *supra*.

130. *See id*.

131. *See* United States v. Giannetta, 909 F.2d 571, 577 (5th Cir. 1990) ("Courts have regularly held that in searches for papers, the police may look through notebooks, journals, briefcases, file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized."); Manno v. Christie, 2008 WL

Agent Daun's conduct is far from the equivalent of briefly perusing or skimming a paper document and then ignoring it once the *out-of-scope* or privileged nature is realized. For IRS-CI Agent Daun's more than three year long digital search, rather than keep *out-of-scope* files/knowledge to herself, she flagrantly shared it with others involved in the investigation. [132]

B. Suppression of all digital evidence is merited based on technical violations of the 30-day search window limitations contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.

Even if the Court finds that no indiscriminate fishing occurred, suppression of *all* digital evidence—or, in the alternative, suppression of digital evidence seized beyond the relevant 30-day search windows—is still an appropriate remedy for the related technical violations of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants.[133] As explained above, the warrants required that (1) some type of minimization procedures be employed, and (2) all data be searched/seized from the forensic images, *etc.* within 30 calendar days of the initial searches used to seize the physical data storage devices. As was discussed in the wholesale suppression subsection, IRS-CI Agent Daun did not complete her search and seizure of data, by copying said data to DVDs and a CD,[134] until September 8,

---

4058016, p. 4 (D.N.J. Aug. 22, 2008) (in context of warrant having **no minimization requirements**, it is "reasonable for [][an agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files").

132. *See* Andresen v. Maryland, 427 U.S. 463, 482 fn. 11.(1976) (noting that when search warrants authorize the seizure of documents, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.").

133. If the Court decides to only suppress digital evidence obtained ***after*** the expiration of the 30-day search window applicable to the N.D.Cal. 08-70460-HRL/PVT warrant, suppression of all evidence obtained under the N.D.Cal. 08-70502-PVT warrant would not be an automatic consequence of suppression, *i.e.*, fruit-of-the-poisonous-tree. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 05 (Dkt. #863-1) (explaining how IRS-CI Agent Daun seized a text file on August 3-4, 2008 (within the 30-day search window applicable to the N.D.Cal. 08-70460-HRL/PVT warrant) leading to the search of storage unit No. A-47). However, the technical violations explained in this subsection still independently apply to all digital evidence seized from the forensic images and virtual machine clones stemming from the search of storage unit No. A-47 under the N.D.Cal. 08-70502-PVT warrant.

134. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from

2009—371 days and 370 days past the respective deadlines.[135] In an opinion addressing an argument nearly identical to the defendant's, the Central District of California suppressed all digital evidence seized by the government after a 60-day forensic search deadline had expired. *See* United States v. Salceda, 2012 U.S. Dist. LEXIS 28211, CR 10-274 CAS (C.D.Cal., Feb. 27, 2012).[136] Similar to *Salceda*, the defendant is requesting suppression of all digital evidence seized after the expiration of the relevant 30-day search windows. *See also* United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Maine 1999), aff'd, 256 F.3d 14 (1st Cir. 2001) (suppression appropriate because the government failed to comply with time limits for reviewing seized computers when those time limits were required by the warrant). Likewise, the defendant is also requesting suppression of *all* seized digital data as a remedy for the violations of the minimization requirements.

In the context of violating a judicially created policy related to the Fourth Amendment, suppression is merited if the violation was the "unattenuated but-for cause of obtaining the evidence." United States v. Hector, 474 F.3d 1150, 1154 (9th Cir. 2007) (paraphrasing Hudson v. Michigan, 547 U.S. 586 (2006)). Just like in *Salceda*, the violation challenged in the present case is a clear unattenuated but-for cause of obtaining all digital evidence beyond the relevant deadlines. Similarly, the minimization violation is a clear

---

apartment No. 1122 and storage unit No. A-47).

135. *See Facts*, Section I, ¶ No. 2, *supra*.

136. After the execution of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants on August 3-4, 2008, Rule 41 was amended in 2009 as follows:

> "Unless **otherwise specified**, the warrant authorizes a later review of the media or information [(*e.g.*, forensic images)] consistent with the warrant[]" and that any time limits set forth in Rule 41 do not refer to "any later off-site copying or review."
>
> Fed. R. Crim. P., 41(e)(2)(B) (emphasis added) (2009).

However, even if the 2009 version of Rule 41 is relevant here, the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants still "otherwise specified," *id.*, that "later off-site copying or review," *id.*, of the defendant's data be completed within 30 days. *See also* United States v. Winther, 2011 U.S. Dist. LEXIS 133799, No. 11-212 (E.D.Pa., Nov. 18, 2011) ("The rule does not prevent a judge from imposing a deadline for the... access to the electronically stored information at the time the warrant is issued." (quoting committee Comments to 2009 Amendments to Rule 41)); United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2008) ("We believe that it is important to preserve the option of imposing [][search] conditions when they are deemed warranted by judicial officers authorizing the search of computers.").

unattenuated but-for cause of obtaining *all* digital evidence, regardless of time deadlines, considering the abrasive, file-by-file "human eye" review was the only type of search conducted by the government from the outset.

Under a Rule 41 violation analysis, which may offer guidance here,[137] suppression is merited for non-constitutional violations of the rule if either (1) "the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule" or (2) "officers acted in 'intentional and deliberate disregard' of a provision in the Rule." United States v. Williamson, 439 F.3d 1125, 1132 (9th Cir. 2006) (citation omitted). The government certainly cannot claim that its first 401-day file-by-file, "human eye" search and thereafter 28-month long file-by-file, "human eye" search were anything but intentional, deliberate, and in plain contradiction to the terms of the warrants. Furthermore, the defendant is certainly prejudiced by the government seizing digital evidence during the 371 days and 370 days following the 30-day deadlines. For example, if the government were to go through its records and collect only that which was isolated (*i.e.*, seized) from the forensic images, *etc.* within the required 30-day search windows, the amount of useable digital evidence would be almost null. Likewise, it certainly created a more abrasive search to allow numerous unqualified agents access to virtual machine clones of the defendant's entire computer system and storage devices for more than a year. It certainly created a more abrasive search to have those agents conduct a "human eye" review while the clones "actually contain[ed] many more files than those that fall within the parameters of the Search Warrant and its attachments."[138]

---

137. The defendant is not alleging a Rule 41 violation. However, the noted case law may provide guidance on whether technical violations of a warrant's terms, as articulated by the issuing magistrate, merits suppression of evidence.

138. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

C. Suppression of all digital evidence is merited considering IRS-CI Agent Daun's seizure of digital data past the 30-day deadlines was done without supporting findings of probable cause.

In addition to preventing the government from engaging in indiscriminate fishing, the directives contained in the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants—requiring that all digital evidence be searched/seized from the forensic images within 30 days unless an extension of time is granted—are intended to ensure that the issuing magistrate renew the probable cause findings upon each granted time extension. Because the government continued to search for and seize evidence after the 30-day search windows had expired, those additional searches/seizures were not supported by findings of probable cause. Even if the government attempts to argue that probable cause did not dissipate after the expiration of the 30-day search windows,[139] and that the issuing magistrate would have therefore found that probable cause continued to exist, "[t]he Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised." United States v. United States District Court, 407 U.S. 297, 317 (1972); *see also* United States v. Mejia, 69 F.3d 309, 320 (9th Cir. 1995) ("If evidence were admitted notwithstanding the officers' unexcused failure to obtain a warrant, simply because probable cause existed, then there would never be any reason for officers to seek a warrant [(or an extension of a warrant for that matter)]."). Because the issuing magistrate did not make a finding of probable cause to search for and seize the defendant's digital data for 371 days beyond the time authorized, all digital evidence seized beyond the 30-day search windows must be suppressed.

D. The government has no valid good-faith claim upon which it can rely in order to erase its Fourth Amendment violations.

The government fails to advance a good-faith claim justifying the above outlined Fourth Amendment violations. To the contrary, the government's own warrant applications and conduct destroy all good-faith arguments that one may attempt to advance in this case.

---

139. *See* United States v. Brewer, 588 F.3d 1165, 1173 (8th Cir. 2009) ("[T]he delay had no effect on the probable cause determination. The computer media at issue here were electronically-stored files in the custody of law enforcement.").

First, the government voluntarily requested that the 30-day search window limitation and minimization requirements be included in the issued warrants.[140] The government cannot now claim that it merely made an innocent mistake in interpreting the warrants or that it was not aware of the very terms it requested and then violated.[141] Second, the government did not seek authority to later ignore the minimization requirements or request extensions of time past the initial 30 days in order to continue its searches and seizures. *Compare* United States v. Mutschelknaus, 592 F.3d 826, 830 (8th Cir. 2010) ("Here, the officers' explicit request for an extension shows a manifest *regard* for the issuing judge's role in authorizing searches, rather than a bad faith attempt to circumvent federal requirements." (internal markup and citation omitted)). Third, if IRS-CI Agent Daun, or the IRS-CI as a whole, lacked the skill or resources to conduct a timely and private forensic analysis, assistance from FBI CART could have been sought. In April of 2010, Nathan Gray, Special Agent in Charge of the FBI-Phoenix Division, said that the multi-agency investigation producing the defendant's arrest was "an excellent example of law enforcement cooperation between the IRS - Criminal Investigations, the U.S. Postal Inspection Service, and the FBI,"[142] therefore, the FBI CART assisting with a proper forensic analysis would not have been a problem. Fourth, contrary to what the October 22, 2012 prosecution report may imply, the Ninth Circuit's string of *CDT* opinions[143] do not objectively affect the government's conduct or decision making in this case. The noted prosecution report has an August 28, 2009 table entry stating

140. *See, e.g., Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122 (Dkt. #566-1) (government's warrant application with "Attachment C" detailing 30-day search window and minimization requirements).

141. *See* Groh v. Ramirez, 540 U.S. 551, 564 (2004) (implying a general rule that if a law enforcement official prepares a warrant, he cannot later note problems in the warrant's text in order to support a claim of qualified immunity).

142. U.S. Attorney's Office, District of Arizona, *press release No. 2010-060 (Rigmaiden, et al.)*, "'Hacker' Indicted In Massive Tax, Mail, And Wire Fraud Scheme," *available at* http://www.justice.gov/criminal/cybercrime/rigmaidenIndict.pdf (last accessed: Feb. 15, 2011).

143. *See* **(1)** United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085 (9th Cir. January 24, 2008), **(2)** United States v. Comprehensive Drug Testing, Inc., 545 F.3d 1106 (9th Cir., September 30, 2008), **(3)** United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir., August 26, 2009), and **(4)** United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir., September 13, 2010) (all interchangeably referred to as "CDT").

that "[d]ue to CDT issues in the 9th Circuit, IRS case agents and FBI agents were instructed to no longer access virtual machines and data."[144] Presumably, the government means that before August 26, 2009, it was relying upon the January 24, 2008 version of *CDT*, *i.e.*, 513 F.3d 1085, to justify its failure to comply with the express time limitations and minimization requirements contained in the relevant warrants. However, that version of *CDT* was vacated by the Ninth Circuit on September 30, 2009[145]—a mere 27 days into the government's initial 401-day fishing exhibition. Likewise, IRS-CI Agent Daun's additional 28-month long fishing exhibition occurred even after the release of the *en banc* August 26, 2009 version of *CDT*. Nevertheless, even if the Court were to consider a hypothetical good-faith reliance on the vacated version, the only prior *CDT* point even remotely relevant to the present case was the Ninth Circuit's use of a (now defunct) backhanded legal analysis[146] intended to expand "plain view" as a means to seize *out-of-scope* digital evidence relating to crimes not listed in a warrant. However, "plain view" is irrelevant to the defendant's Fourth Amendment challenges considering the government has identified no *out-of-scope* evidence it plans to use in support of new charges or investigations.[147] In other words, the "plain view" doctrine is entirely separate from the Fourth Amendment question at issue here, *i.e.*, whether it was illegal for the government to conduct a fishing exhibition while violating the express terms

---

144. *Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (Dkt. #929-1, p. 9).

145. *See CDT*, 545 F.3d 1106 ((Rehearing, *en banc*, granted and, as of September 30, 2008, "[t]he three-judge panel opinion shall not be cited as precedent by or to any court of the Ninth Circuit.").

146. *See CDT*, 513 F.3d at 1112 fn. No. 48 ("We do not reach the government's argument that the "plain view" exception to the warrant requirement justified seizure of the intermingled evidence, because the [blanket, indiscriminate seizure and viewing of all digital data] evidence fell within the scope of the search warrant." [addressing warrant with **no** minimization requirements or time limits]), *vacated*, 545 F.3d 1106; *but see CDT*, 579 F.3d at 1006 (Framing the dispute as a "plain view" issue, finding that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.").

147. However, the government does seem to at least imply that it will use *out-of-scope* data seizures as evidence in *other* cases. *See Second Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 088 (Dkt. #821-5) ("Searches for evidence to be used in **this case** are being limited to the materials indexed in the February 25, 2010, discovery." (emphasis added)). If the government does have this plan, it will have to deal with the defendant's *pro se* Fourth Amendment defense once again.

of the noted warrants' "Computer Search Protocol" by using multiple sets of "human eyes" to indiscriminately rummage through personal, private and privileged *out-of-scope* files for over three years while failing to disregard data reflective of no crime at all. Even the vacated *CDT* opinion held that "a Fourth Amendment violation could still occur if the government did not comply with the warrant protocol[.]"[148] Notably, the *CDT* case as a whole did **not** involve the type of minimization requirements and time limitations contained in the warrants at issue in the present case. Nor did the *CDT* agents review, share, and discuss a multitude of private data relating to no crimes at all. Contrary to what IRS-CI Agent Daun and the other case agents may have believed, there was nothing prior to the August 26, 2009 *CDT* opinion allowing the government to engage in protracted, indiscriminate, exploratory rummaging into private *out-of-scope* digital data while ignoring a warrant's express terms not to do so. The Ninth Circuit did not somehow "reinstate" the Fourth Amendment for digital searches on August 26, 2009 or even on September 30, 2008. To the contrary, the Fourth Amendment was in play all along.

III. Conclusion: Exclusion is an appropriate remedy and all illegally obtained evidence and derivative evidence must be suppressed.

*. In light of the new evidence provided to the defense by the government on June 21, 2012 and on October 22, 2012, the following conclusion supplements, corrects, and supersedes the conclusion contained in the defendant's *Motion To Suppress* (Dkt. #824), *Memorandum Re: Fourth Amendment Violations (re: N.D.Cal. 08-70460-HRL/PVT)* (Dkt. #830-1), *Conclusion*, Section III—however, only applicable to arguments relating to searches/seizures of digital evidence as raised in this filing, Section II, *supra*.[149]

As a remedy for any or all of the herein explained violations, and in order to deter the government from engaging in similar misconduct in the future, the defendant respectfully requests that the Court suppress the following evidence obtained illegally in this case:

148. *CDT*, 513 F.3d at 1107 fn. No. 44, *vacated*, 545 F.3d 1106.

149. In other words, the *Conclusion* contained in *Memorandum Re: Fourth Amendment Violations (re: N.D.Cal. 08-70460-HRL/PVT)* (Dkt. #830-1), Section III, remains applicable to suppression arguments contained in Sections II(A) and (B) of Dkt. #830-1—*i.e.*, relating to Fourth Amendment violations not involving searches/seizures of digital evidence.

EVIDENCE TABLE

#	Evidence sought to be suppressed:
1	Wholesale suppression of all physical effects—which encompasses *all* digital data as *fruits-of-the-poisonous-tree*—seized under the N.D.Cal. 08-70460-HRL/PVT (apartment No. 1122) and 08-70502-PVT (storage unit No. A-47) warrants, as a sanction for the government's fishing exhibition with respect to searched/seized digital evidence;
2	Suppression of all *digital evidence* seized under the N.D.Cal. 08-70460-HRL/PVT (apartment No. 1122) and 08-70502-PVT (storage unit No. A-47) warrants, both before **and** after the 30-day search window, as either a sanction for the government's fishing exhibition with respect to searched/seized digital evidence or as a sanction for one or both technical violations of the warrants, *i.e.*, 30-day search window and/or minimization;
3	Suppression of data isolated (*i.e.*, seized) from government forensic images and virtual machine clones of physically seized data storage devices and encrypted virtual drives, but applicable to data seized **after** the first 30 days following the in-person search of apartment No. 1122 (N.D.Cal. 08-70460-HRL/PVT warrant), [*e.g.*, data contained on the September 8, 2009 DVDs and CD referenced in IRS-CI Agent Daun's "Computer Forensic Report," data seized after the first 30 days into the government's initial 401-day fishing exhibition, and data seized during the government's subsequent 28-month fishing exhibition] as a sanction for the 30-day search window technical violations of the relevant warrants;
4	Suppression of seized physical data storage devices and encrypted virtual drives that contain many more files than those falling within the scope of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants;
5	Suppression of government forensic hard drive images / copies / virtual machine clones of seized physical data storage devices and encrypted virtual drives that contain many more files than those falling within the scope of the N.D.Cal. 08-70460-HRL/PVT and 08-70502-PVT warrants;
6	All derivative evidence, *i.e.*, fruits-of-the-poisonous-tree, stemming from primary evidence sought to be suppressed (*see* Nos.1-5 above) including, but not limited to, all evidence seized pursuant to the N.D.Cal. 08-70502-PVT warrant, N.D.Cal. 08-70503-PVT warrant, E.D.Cal. 08-SW-0586-EFB warrant, D.Ariz. 08-3397MB-LOA warrant, D.Ariz. 08-3399MB-LOA warrant, D.Ariz. 08-3401MB-LOA warrant, D.Ariz. 08-3403MB-LOA warrant, D.Ariz. 08-3402MB-LOA warrant, D.Ariz. 08-3398MB-LOA warrant, D.Ariz. 08-6038MB-DKD warrant, D.Ariz. 09-7124MB-ECV warrant, and all other warrants;

This filing was drafted and prepared by the *pro se* defendant, however, he authorizes his shadow counsel, Philip Seplow, to file this filing on his behalf using the ECF system. The defendant is appearing *pro se* and has never attended law school. The defendant's filings, however inartfully pleaded, must be liberally construed and held to less stringent standards than formal pleadings drafted by lawyers. *See* Haines v. Kerner, 404 U.S. 519, 520 (1972).

LRCrim 12.2(a) requires that the undersigned include the following statement in all

motions: "Excludable delay under 18 U.S.C. § 3161(h)(1)(D) will occur as a result of this motion or of an order based thereon."

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

Respectfully Submitted: May 22, 2013

PHILP SEPLOW, Shadow Counsel, on behalf of DANIEL DAVID RIGMAIDEN, Pro Se Defendant:

s/ Philip Seplow
Philip Seplow
Shadow Counsel for Defendant.

CERTIFICATE OF SERVICE

I hereby certify that on: May 22, 2013 I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Taylor W. Fox, PC
Counsel for defendant Ransom Carter
2 North Central Ave., Suite 735
Phoenix, AZ 85004

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

By: s/ Daniel Colmerauer
(Authorized agent of Philip A. Seplow, Shadow Counsel for Defendant; See ECF Proc. I(D) and II(D)(3))